

**IN THE SPECIFICATION**

OCT 28 2004



Please delete the paragraph beginning on page 2, line 1 in its entirety.

**RECEIVED**

NOV 5 2004

**Group 2100**

Please amend the paragraph beginning on page 2, line 33 as follows:

--The computer system includes a central processing unit, a hard disk, and a nonvolatile ~~random access~~ memory, such as a random access memory, a read-only memory or flash memory device. The Extensible Firmware Interface is a ROM-based operating system (i.e. stored in the read-only memory or flash random access memory) that provides disk operating system (DOS) functionality for the computer system, and is controlled by the BIOS.--

Please amend the paragraph beginning on page 3, line 8 as follows:

--The present method ~~comprises~~ includes the following steps: A command shell of the Extensible Firmware Interface is modified to include a command that operates to copy the boot sector of the hard disk to the nonvolatile ~~random access~~ memory. The modified Extensible Firmware Interface is stored in the nonvolatile ~~random access~~ memory. When the computer system is initialized (booted), a boot sector of the hard disk is copied to the nonvolatile ~~random access~~ memory. The boot sector of the hard disk is automatically read back from the nonvolatile ~~random access~~ memory on each boot, which bypasses the boot sector access of the hard disk during system initialization.--

Please amend the paragraph beginning on page 3, line 16 as follows:

--An extra field may be added to a BIOS SETUP routine, which is part of the BIOS, that allows a user to enable or disable reading of the boot record from nonvolatile ~~random access~~ memory on boot. In implementing this aspect of the present method, the BIOS SETUP routine is run, and the user is prompted to enable or disable reading the boot record from nonvolatile ~~random access~~ memory on boot. The use of the BIOS SETUP routine allows a user to recover if he or she changes the boot disk or intentionally changes the boot disk's boot record to change the operating system or partition of the hard disk.--

Please amend the paragraph beginning on page 3, line 24 as follows:

--The method may also be modified to require entry of a security signature to prevent unauthorized updating of the stored boot sector. In implementing this aspect of the present invention, the command shell of the Extensible Firmware Interface is modified to include ~~a command~~ a security signature input field. At the appropriate time during execution of the Extensible Firmware Interface the security signature input field is displayed to a user. The required signature is then input by the user prior to updating the stored boot sector.--

Please amend the paragraph beginning on page 6, line 6 as follows:

--The software 20 or firmware 20 that implements the method 20 may also be modified to require entry of a security signature to prevent unauthorized updating of the stored boot sector. In implementing this aspect of the present invention, the command shell of the Extensible Firmware Interface 15 is further modified 31 to include ~~a command~~ a security signature input field. At the appropriate time during execution of the Extensible Firmware Interface 15 the security signature input field is displayed 32 to a user. The required signature is then input 33 by the user prior to updating the stored boot sector.--

Please amend the paragraph beginning on page 4, line 14 as follows:

--The computer system 10 ~~comprises~~ includes a central processing unit (CPU) 11, which is coupled to a hard disk 12, a read-only memory (ROM) 13, and a nonvolatile ~~random access~~ memory, for example, a nonvolatile random access memory (NVRAM) 14, also known as flash memory 14. The computer system 10 also ~~comprises~~ includes an Extensible Firmware Interface (EFI) 15 which is a ROM-based operation system (i.e., stored in the read-only memory 13) that provides disk operating system (DOS) functionality for the computer system 10, along with a basic input and output (BIOS) 16.

--

Please amend the paragraph beginning on page 4, line 34 as follows:

--The basic input and output system 16, or BIOS 16, is a firmware program that is stored in the nonvolatile random access memory 14 (or flash memory 14). The BIOS 16 brings up the computer system 10 when it is turned on. The Extensible Firmware Interface 15 is controlled by the BIOS 16 and executes before any other operating systems are loaded or access is allowed to the hard disk 12. --

Please amend the paragraph beginning on page 5, line 3 as follows:

--The BIOS 16 determines what the computer can do without accessing programs from the hard disk 12 or other media. The BIOS 16 contains code required to control, for example, the keyboard, display screen, disk drives, serial communications, ~~for example~~, along with certain other functions, depending upon the computer system 10. --

Please amend the paragraph beginning on page 5, line 16 as follows:

--Fig. 2 is a flow diagram that illustrates an exemplary method 20 in accordance with the principles of the present invention for providing virus protection for the computer system 10. The method 20 is designed to protect and remedy potential viruses that are loaded onto the computer system 10. --

Please amend the paragraph beginning on page 5, line 20 as follows:

--The method 20 comprises software 20 and preferably firmware 20 that is used in conjunction with a computer system 10 comprising a central processing unit (CPU) 11, a hard disk 12, a nonvolatile memory (NVRAM) 14, a basic input and output system (BIOS) 16, and an Extensible Firmware Interface 15. The software 20 or firmware 20 is stored in and is executed from the nonvolatile memory (NVRAM) 14 (or ROM 13) of the computer system 10. The method 20 comprises the following steps. --

Please amend the paragraph beginning on page 5, line 35 as follows:

--An extra field may be added 25 to a BIOS SETUP routine 17, which is part of the BIOS 16, that allows a user to enable or disable reading of the boot record from nonvolatile random access memory 14 on boot. In implementing this aspect of the

present method 20, the BIOS SETUP portion of the BIOS 16 is run 26, and the user is prompted to enable 27 or disable 28 27 reading of the boot record from nonvolatile random access memory 14 on boot. The use of the BIOS SETUP routine 17 allows a user to recover if he or she changes the boot disk or intentionally changes the boot disk's boot record to change the operating system or partition of the hard disk 12. --

Please amend the paragraph beginning on page 6, line 6 as follows:

--The software 20 or firmware 20 that implements the method 20 may also be modified to require entry of a security signature to prevent unauthorized updating of the stored boot sector. In implementing this aspect of the present invention, the command shell of the Extensible Firmware Interface 15 is further modified 31 to include a ~~command~~ a security signature input field. At the appropriate time during execution of the Extensible Firmware Interface 15 the security signature input field is displayed 32 to a user. The required signature is then input 33 by the user prior to updating the stored boot sector. --